Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1417 05/04/12

~ Hoarder Buries Himself ~ CISPA Opposition Grows! ~ Xbox & Win 7 Ban!

-* Why CISPA Is Worse Than SOPA *-
-* Website Address Revolution on Hold! *-
-* Amazon, Texas Reach Deal in Sales Tax Spat *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

I'm still waiting for a few good things to happen these days! It seems like tragedy and bad luck has a vice-like grip on me, with no chance to get loose. The list of misfortune has continued to grow. Last week, it was the lack of time due to the continuing "saga" of red tape regarding my father's estate, and my wife's mother's affairs after the fire. And then, we took our ailing oldest dog to the vet to get an update on her condition because she was getting worse.

So, the legal affairs continue to worsen as far as family members' lack of cooperation and communication - in both families. And, earlier this week, our dog got even worse; and we could tell that she wasn't going to have much quality of life left. So, seeing her struggle early in the week, we decided that it was time. It was rough for my wife and I to watch her pass away, but we were there for her right to the end. What more could we have done? So, the house is a little empty at the moment without her presence, but she will always be with us in many other ways. 16 years she was with us - a lot of great memories will stay with us.

So, I'm still not mentally all there at the present, so my thoughts for other things aren't in focus right now. I'm sure you'll give me a little leeway for a bit until things somehow get back into focus.

Until next time...

=~=~=~=

->In This Week's Gaming Section - Hoarder Buried Himself in Atari Games!
""""""""""""""""""""""""""""""""" $99 Xbox with Subscription!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Hoarder Buried Himself in Atari Games and Bobble Heads

Lee Shuer’s hoarding began a decade ago as he began collecting Atari video games then progressed to vintage art work and musical instruments.

But soon, his apartment was overflowing with bobble heads, collectibles and anything he could get "free or a good deal."

"It got to the point where more is better," said Shuer, now 37, of Easthampton, Mass. "Eventually, they spilled off the shelves, onto the floor, down the hall, into the bedroom, off the bed - you could see the tide flow."

Shuer’s acquisitions became part of his identity and self-esteem.

"If I had more fun and more toys, people might actually like me," he said. "If I had enough things to play with, they might come hang out."

When he finally met his future wife and they had to clean out the clutter to move in to a new home, she was horrified by the volume of things and begged him to call for help.

Shuer did, and this week he is one of the key presenters at the 14th Annual Hoarding and Cluttering Conference, sponsored by the San Francisco Mental Health Association. There, both clinicians and hoarders will attend an array of workshops on best practices and new treatments.

"I give my wife a lot of credit," he told ABCNews.com. "If it wasn’t for her, I wouldn’t be talking to you now."

After participating in a study at Smith College in 2005 with pioneering hoarding expert Randy O. Frost, Shuer joined a hoarding task force and began to help others.

"Hoarding has been around a long time, all the way back to the 14th century," said Frost, psychology professor and co-author of the 2011 book, "Stuff: Compulsive Hoarding and the Meaning of Things."

In one of the most famous cases in the 1940s, the Collyer brothers were found dead in their New York City apartment under 100 tons of trash, including human pickled organs, the chassis of an old Model T, 14 pianos, hundreds of yards of unused silks and fabric, the folding top of a horse-drawn carriage, and more than 25,000 books.

Frost identified the three features of hoarding: excessive acquisition, difficulty discarding and disorganization. He developed the "Buried in Treasures" self-help program that gave Shuer his life back.

Compulsive hoarding is strongly associated with obsessive compulsive disorder (OCD), a condition that affects about 4 million Americans, according to the OCD Foundation. About 25 to 40 percent of those with OCD have hoarding symptoms.

Psychiatrists are now hopeful that hoarding will get its own category in the Diagnostic and Statistical Manual of Mental Disorders V this year, distinguishing it from obsessive-compulsive disorder.

Hoarding can lead to serious health or safety dangers and threaten relationships with family and friends.

The disorder is diagnosed when a person experiences significant distress and/or impairment as a result of their hoarding.

Homes on television shows like TLC's "Hoarding: Buried Alive" can have infestations of rodents or insects. Hoarders are unable to entertain guests, prepare food or find their possessions.

"It's difficult to actually get an estimate of how many people are hoarders," said Julie L. Pike, who has appeared on the show and is a psychologist at the Anxiety Disorder Treatment Center in North Carolina.

"There is so much shame and so much hiding around it," she said.

Often hoarders do not seek help until it is too late - when they have lost their children, their home or a spouse.

In one of the most serious cases of hoarding on the reality show, Pike helped a woman whose home was infested with a nest of black widow spiders and cockroaches. Uncapped insulin needles and dirty incontinence pads were strewn everywhere.

"The exterminator said it was the worst infestation he'd seen in 23 years," said Pike.

$99 Xbox with Subscription Another Great Microsoft Idea

The Verge is reporting that Microsoft is getting ready to start selling a $99 Xbox 360 as long as owners commit to a two-year data plan.

ZDNet reports that the monthly subscription to Xbox Live, which is the online network for the Xbox, would ring in at $15 per month. The report mentions that users would get access to the current level of Xbox Live Gold membership benefits and also a few other features for entertainment and sports. As long as the subscription comes with enough value added channels and apps to offset the $15 per month fee, like a free Hulu or Netflix subscription, the deal would be well worth it. It's a great move for Microsoft.

Ars Technica reports, the Xbox would move to more of an entertainment hub than a game machine, which it already is in many homes. The big deal with a $99 Xbox is how Microsoft would subsidizing the unit with online subscriptions, and like ZDNet points out, gets handled exactly like a mobile phone right down to the early termination fee. The move would represent a major shift in the video game industry.

The video game world could be starting to skew into total home entertainment, which only makes sense given the popularity of streaming. Of course, Netflix is already available on the Xbox 360, and so is the new streaming partnership courtesy of Vudu and UltraViolet. As buyers look for a low purchase price, a relatively cheap Xbox combined with a Kinect sensor is a great deal, and it looks even better when quality monthly content is factored in.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

U.S. House Passes CISPA

The United States House of Representatives has voted to pass the controversial Cyber Intelligence Sharing and Protection Act (CISPA), talk of which has swept the Internet over the past few weeks. The House vote was moved up to Thursday night, and CISPA passed as 248 members of Congress voted for the bill and 168 voted against. The bill is sponsored by Representatives Mike Rogers (R-Michigan) and Dutch Ruppersberger (D-Maryland), and it now faces further modifications in the Senate if it is to avoid being vetoed by the White House. President Barack Obama has indicated that he intends to veto the bill if it makes it to his desk, noting that as it is written now, the legislation would allow "broad sharing of information with governmental entities without establishing requirements for both industry and the government to minimize and protect personally identifiable information." The American Civil Liberties Union issued a statement following the vote. "Cybersecurity does not have to mean abdication of Americans online privacy," said ACLU legislative counsel Michelle Richardson. "As we ve seen repeatedly, once the government gets expansive national security authorities, there s no going back. We encourage the Senate to let this horrible bill fade into obscurity."

Why CISPA Is Worse Than SOPA

Following the SOPA/PIPA uproar that splashed across the Internet earlier this year, we now have another cyber-security bill that threatens American Web browsing privacy, the Cyber Intelligence Sharing and Protection Act, otherwise known as CISPA.

The House of Representatives passed the bill Thursday evening, moving the legislation closer to law. The bill is stalled in the Senate and President Obama has said he would veto the law if it made it to his desk. Even so, activists and observers on the Internet saw how far SOPA got and backers expect it to pass, says ProPublica. Protestors also saw how far education, blogging and general Internet awareness campaigns got them in the fight against it. Many see CISPA as just as bad, if not worse than the previous cyber security bills, and they're pushing back on it.

Before doing any protesting, the techies first clarified what makes CISPA the new SOPA. It's actually not exactly the new SOPA, as ProPublica's very complete explainer, points out. "SOPA was about intellectual property; CISPA is about cyber security, but opponents believe both bills have the potential to trample constitutional rights," writes ProPublica's Megha Rajagopalan. But, both have to do with the way you use the Internet and

both threaten user privacy. This bill has nothing to do with copyright and online intellectual property. It would do more than just shutdown your favorite overseas pirates. But like SOPA, in the name of some loftier goal - in SOPA's case copyright, in CISPA's case cyber-security - CISPA gives the government your Internet. With SOPA, this meant censoring the Internet. CISPA, however, gives companies many Americans use, like Facebook and Twitter the ability to hand over your information to any government agency.

And here's where many decided CISPA was worse than SOPA. Both the Center for Democracy and Technology and the Electronic Frontier Foundation agree CISPA's language is far too broad. As Gizmodo points out in its useful explainer, the law's vague language gives the government a lot of leeway here. Per Gizmodo's Sam Biddle:

CISPA says companies need to give up your information only in the face of a "cyber threat." So, what is a "cyber threat"? Nobody really knows! The bill defines it as "efforts to degrade, disrupt, or destroy government or private systems and networks." In other words, trying to do bad stuff on the internet, or even just talking about it. Ideally, this would be narrowed to specific malicious LulzSec stuff like DDoS attacks, but it's not. It can be almost anything!

Over at TechDirt you can read the broad reasons the government says it needs information seizure, some of which got added to the bill last minute. "The government would be able to search information it collects under CISPA for the purposes of investigating American citizens with complete immunity from all privacy protections as long as they can claim someone committed a 'cybersecurity crime'," writes TechDirt's Leigh Beadon. "Basically it says the 4th Amendment does not apply online, at all." And the government has structured the bill so it won't have much oversight, explains the Sunlight Foundation's John Wonderlich. He points to this section of the bill, which exempts CISPA from the Freedom of Information Act. "The FOIA is, in many ways, the fundamental safeguard for public oversight of government's activities," he writes. "CISPA dismisses it entirely, for the core activities of the newly proposed powers under the bill."

The other part that's scarier than SOPA is that it might actually pass. Many have pointed out that a divided house passed the bill 248-168, showing this is something both parties agree on. And while the House is united, the Internet this time around is not, with big Web juggarnauts that opposed SOPA, supporting CISPA. Facebook, for example, levied its support in a company blog post. "Importantly, HR 3523 would impose no new obligations on us to share data with anyone - and ensures that if we do share data about specific cyber threats, we are able to continue to safeguard our users private information, just as we do today," wrote Facebook s vice president of public policy, Joel Kaplan. ProPublica has put together a chart comparing the points of view of key players, showing how they come out on SOPA versus CISPA. Wikimedia, which led the controversial Wikipedia blackout, for example, is currently undecided on the topic. The divide, as Rajagopalan explains, is happening this time around because this bill would help these companies deal with real threats better. And there's a whole slew of other big name non-Internet companies, like Boeing and Verizon, supporting the legislation, too. (Here's the full list of their letters of support.)

But many critics don't even think the bill would make us safer. "Some cyber security specialists note that neither CISPA nor other cyber security bills in Congress would compel companies to update software, hire outside

specialists or take other measures to preemptively secure themselves against hackers and other threats," writes. And even if it has minimal net-benefits, it’s definitely not worth all the privacy we would give up, which is the ACLU’s position. That group came out with the following statement. "CISPA goes too far for little reason. Cybersecurity does not have to mean abdication of Americans online privacy. As we ve seen repeatedly, once the government gets expansive national security authorities, there s no going back. We encourage the Senate to let this horrible bill fade into obscurity," said ACLU legislative counsel Michelle Richardson after the house vote.

Even if the bill passes the Senate, where there is no corresponding bill at the moment, Obama has already issued a veto threat, as ArsTechnica points out. But the paranoid note that Obama’s veto rhetoric hasn’t been all that reliable. "Dear Obama: Your rhetoric on NDAA, Gitmo & Wall Street proved empty & false. We’ll believe a #CISPA veto when we see it. Love, the Internet," tweeted an Anonymous Twitter handle, @YourAnonNews.

Opposition Grows to CISPA ’Big Brother’ Cybersecurity Bill

Last-minute opposition to the CISPA, which has been criticized as a "Big Brother" cybersecurity bill, is growing as the U.S. House of Representatives prepares for a vote this week.

Rep. Ron Paul, the Texas Republican and presidential candidate, warned in a statement and YouTube video today that CISPA (PDF) represents the "latest assault on Internet freedom." Paul warned that "CISPA is Big Brother writ large," and said that he hopes that "the public responds to CISPA as it did to SOPA back in January."

In addition, 18 Democratic House members signed a letter (PDF) this afternoon warning that CISPA "does not include necessary safeguards" and that critics have raised "real and serious privacy concerns." The number of people signing an anti-CISPA petition is now at more than 718,000, up about 100,000 from a week ago.

Excerpts from the Cyber Intelligence Sharing and Protection Act:

"Notwithstanding any other provision of law, a self-protected entity may, for cybersecurity purposes - (i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such self-protected entity; and (ii) share such cyber threat information with any other entity, including the Federal Government...

The term ’self-protected entity’ means an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself."

CISPA would permit, but not require, Internet companies to hand over confidential customer records and communications to the U.S. National Security Agency and other intelligence and law enforcement agencies.

It’s hardly clear, however, that this wave of opposition will be sufficient.

CISPA - also known as the Cyber Intelligence Sharing and Protection Act - has 113 congressional sponsors. Instead of dropping off as criticism

mounted, which is what happened with the SOPA protests in January, more continue to sign up, with six new sponsors adding themselves in the last week.

Rep. Mike Rogers (R-Mich.), chairman of the House Intelligence Committee, said today that he remains confident that the CISPA will be approved this week.

"Chairman Rogers continues to have an open door and continues to work to address privacy concerns as the bill moves toward the floor," a House Intelligence Committee spokesman told CNET this afternoon.

Foes of CISPA are hoping to submit amendments that, they believe, would defang the most objectionable portions.

The House GOP leadership has scheduled a vote on CISPA for this Friday. Proposed amendments to CISPA are required to be submitted to the House Rules committee by 1:30 p.m. PT tomorrow.

Rep. Zoe Lofgren, a California Democrat whose district encompasses the heart of Silicon Valley, said today: "I cannot support it in its current form. I made suggestions to improve the bill to safeguard the privacy and due process rights of all Americans." (Lofgren posted (PDF) a longer list of concerns on her Web site.)

What sparked the privacy worries - including opposition from the Electronic Frontier Foundation, the American Library Association, the ACLU, and the Republican Liberty Caucus - is the section of CISPA that says "notwithstanding any other provision of law," companies may share information "with any other entity, including the federal government."

By including the word "notwithstanding," CISPA's drafters intended to make their legislation trump all existing federal and state civil and criminal laws. It would render irrelevant wiretap laws, Web companies' privacy policies, educational record laws, medical privacy laws, and more. (It's so broad that the non-partisan Congressional Research Service once warned (PDF) that using the term in legislation may "have unforeseen consequences for both existing and future laws.")

A position paper on CISPA from Rogers and Ruppersberger says their bill is necessary to deal with threats from China and Russia and that it "protects privacy by prohibiting the government from requiring private sector entities to provide information." In addition, they stress that "no new authorities are granted to the Department of Defense or the intelligence community to direct private or public sector cybersecurity efforts."

During a town hall meeting that CNET hosted last week in San Francisco, Jamil Jaffer, senior counsel to the House Intelligence Committee, said the protests ignored the fact that the bill was approved by a bipartisan committee majority back in December.

"There's no secret agenda here. It's only 19 pages," Jaffer said. "You don't need to be a lawyer to read this bill."

Mozilla First Silicon Valley Heavyweight To Oppose CISPA

Thousands of people oppose the controversial Cyber Intelligence Sharing

and Protection Act (CISPA), including the Obama Administration and Anonymous. The bill, which was recently passed by the United States House of Representatives, looks to give businesses and the federal government legal protection to share cyber threats with one another in an effort to prevent online attacks. Internet privacy and neutrality advocates feel as if the bill does not contain enough limits on how and when private information can be monitored. Numerous technology companies such as Microsoft, Apple, Facebook, IBM, Intel and Oracle have voiced their support for the bill. Mozilla on Tuesday, however, took a stand and announced its opposition against CISPA.

While we wholeheartedly support a more secure Internet, CISPA has a broad and alarming reach that goes far beyond Internet security, the company s privacy and public policy lead said to Forbes. The bill infringes on our privacy, includes vague definitions of cybersecurity, and grants immunities to companies and government that are too broad around information misuse. We hope the Senate takes the time to fully and openly consider these issues with stakeholder input before moving forward with this legislation.

Mozilla s Mountain View neighbor, Google, has yet to make its stance known, and is one of the last tech firms to do so. We think this is an important issue and we re watching the process closely but we haven t taken a formal position on any specific legislation, a company spokesperson said. The Internet giant has previously spoken out about the Stop Online Privacy Act (SOPA) and Protect Intellectual Property Act (PIPA), even going as far as censoring its homepage and urging visitors to oppose the bill.

Amazon, Texas Reach Deal To Settle Sales Tax Spat

Online retailer Amazon.com reached an agreement with Texas officials Friday to settle a sales tax dispute by expanding operations in the state and starting to collect sales taxes.

The deal comes less than a year after Amazon shut down a distribution center in Irving to protest a $269 million tax bill sent by Texas Comptroller Susan Combs in 2010.

Combs and Amazon said in a joint statement that the settlement calls for the company to bring at least 2,500 jobs and $200 million in capital investments. The company will begin collecting and paying sales tax July 1. Last year Gov. Rick Perry denounced Comb’s decision to collect the taxes, saying it would cost Texas jobs and discourage companies from moving to Texas.

The announcement came the day after Amazon posted first-quarter profits that blew away analysts’ estimates and boosted the company’s stock.

The move is a dramatic reversal for Amazon, which has fought hard across the country against being forced to collect state sales taxes. Texas law requires companies with a physical presence in Texas to collect sales tax. After Combs concluded last year that the company owed $269 million in uncollected sales taxes, Amazon closed down the warehouse and argued it did not qualify under the law. The deal announced Friday settled that dispute.

In a Securities and Exchange Commission filing Friday, Amazon said it still believes it never owed Texas any taxes but had nevertheless reached a settlement. The national fight over whether online retailers should have to collect state and local sales tax just the same way local merchants must remains unresolved.

Local shops argue online retailers have an unfair price advantage because they are not required to collect taxes on behalf of the state that in Texas can reach 8.5 percent of the sales price. Combs and Amazon’s Vice President of Global Public Policy Paul Misener both committed to working toward a national solution to solving that problem.

"This is an important step in leveling the playing field in Texas," Combs said in a statement. "However, Congress should enact federal legislation that will give states access to revenues that are already due, which would resolve this issue fairly for all retailers and all states."

Amazon has said in the past that the complexity of the state and local sales tax system makes it impossible for big online retailers to accurately collect sales tax and that it supports a national, standardized approach.

"We appreciate Comptroller Combs working with us to advance federal legislation," Misener said. "We strongly support the creation of a simplified and equitable federal framework, because Congressional action will protect states’ rights, level the playing field for all sellers, and give states like Texas the ability to obtain all the sales tax revenue that is already due."

The Alliance for Main Street Fairness, which has fought to force online retailers to collect state and local tax, also welcomed the agreement and called for Congress to enact a national solution.

Sales Tax Deal with Texas is Amazon’s Latest

Amazon.com agreed to begin collecting sales tax in Texas on Friday, forging a deal that promises to bring more jobs to the southern U.S. state and as the online marketer lost another round in a series of state-by-state sales tax battles.

The agreement, to take effect on July 1 for Texas’ 6.25-percent sales tax, follows another accord reached with Nevada earlier in the week to begin collecting that state’s 8.1 percent sales tax on January 1, 2014.

Amazon rings up an estimated 20 percent of all U.S. online retail sales, making it the country’s largest online retailer.

Most online purchases are free of sales tax, which has given the company an edge over traditional, bricks-and-mortar retailers that do collect sales tax.

As online sales have grown, and municipal budgets have tightened, states have been pushing hard to capture more e-tail sales tax revenue.

Under federal law, retailers with physical facilities in a state can be forced by the state to collect sales tax on purchases made by a resident of that state. That includes e-tailers with distribution centers.

E-tailers without physical facilities in a state need not collect the tax.

As Amazon has grown, it has needed more distribution facilities, and in the past few years has parlayed the promise of new facilities in exchange for the best tax terms possible with states across the country.

The importance of that advantage was clear when Amazon pulled up stakes in Texas last fall, shutting down its distribution hub at the Dallas-Fort Worth airport after Texas State Comptroller Susan Combs sent Amazon a $269 million bill covering sales taxes it did not collect from 2005 to 2009.

In exchange for Amazon’s promise to collect future taxes, create at least 2,500 jobs and make at least $200 million in capital investments in the Lone Star state, Combs is dropping the demand for back taxes.

Texas will bring to six the number of states where Amazon currently collects sales tax.

According to its website, it already collects sales tax in five of the 50 states - Kansas, Kentucky, New York, North Dakota and Washington - on purchases made by people who live in those states. Those are the five states where it has physical facilities or affiliated sellers and no agreement with state governments exempting Amazon from collecting sales tax.

A comprehensive federal solution to the question of which companies must collect sales tax on online purchases has yet to reach a vote in Congress.

In announcing the deal with Texas, Amazon’s Vice President of Global Public Policy, Paul Misener reiterated the company’s support for a national solution.

On Thursday, Amazon reported net sales of $13.18 billion for the first quarter of 2012, up 34 percent from the same quarter last year, with net income of $130 million.

Website Address ’Revolution’ on Hold

The Internet domain name "revolution" was on hold Friday due to a flaw that let some aspiring applicants peek at unauthorized information at the registration website.

It remained unclear when the Internet Corporation for Assigned Names and Numbers (ICANN) would resume taking applications from those interested in running new generic top-level domains (gTLDs) online.

ICANN cancelled a Monday event at which details of who applied for which new domains were to be revealed after a system problem delayed the close of the application window. The original domain name application deadline of Thursday was extended to April 20.

"We have learned of a possible glitch in the TLD application system software that has allowed a limited number of users to view some other users’ file names and user names in certain scenarios," ICANN chief operating officer Akram Atallah said in an online message posted on April 12.

"Out of an abundance of caution, we took the system offline to protect applicant data... We are examining how this issue occurred and considering appropriate steps forward."

In January, ICANN began taking applications from those interested in operating Internet domains that replace endings such as .com or .org with nearly any acceptable words, including company, organization or city names.

Outgoing ICANN president Rod Beckstrom has championed the change as a "new domain name system revolution."

The new system will allow Internet names such as .Apple or .IMF or .Paris.

ICANN says the huge expansion of the Internet, with two billion users around the world, half of them in Asia, requires the new names.

"When the application system reopens, users will be able to review their applications, including those already submitted, to assure themselves that their information remains as they intended," Atallah said Thursday in an update.

"We expect that demands on the system will be high when it reopens, and we are enhancing system performance as part of our preparations for the reopening."

More than 25 global bodies have expressed concern about the possible "misleading registration and use" of their names.

They fear it could cause confusion about their Internet presence and force them to spend huge amounts on "defensive registration" to stop cybersquatters, who buy up names and try to sell them at an inflated price, and fraudsters.

Registration costs $185,000 with a $25,000 annual fee after that.

ICANN insists, however, that safeguards are in place to protect names of established companies and groups.

Google Raises Bounty on Software Bugs

Google on Monday raised to $20,000 its bounty on software bugs that hackers could exploit for cyber attacks on the Internet giant’s online services.

The maximum reward for exposing a vulnerability that would let an intruder’s code get up to mischief in a Google datacenter was ramped up from the $3,133.70 payout set when the bounty program launched in November of 2010.

"When we get more bug reports, we get more bug fixes," Google security team manager Adam Mein told AFP. "That is good for our users; that is good for us."

Google has paid out approximately $460,000 since it established the Vulnerability Reward Program.

Of the 11,000 software flaws reported to Google, more than 780 qualified for rewards ranging from $300 to the maximum, a figure selected because the digits translate into a technical term in a hacker programming language.

The bounty was raised to inspire software savants to hunt for difficult-to-find, and potentially perilous, bugs hidden deep in programs, according to Mein.

"We want them to know the reward is there for them if they find the most severe bugs," Mein said.

Bugs found in more sensitive services such as Google smartphone "Wallet" software tends to merit more generous rewards.

People vying for bounties have tended to be computer security professionals; engineering students honing their skills, and website operators, according to Google.

UK Court Tells Service Providers: Block Pirate Bay

Britain’s High Court has ordered the country’s Internet service providers to block file-sharing website The Pirate Bay, the U.K.’s main music industry association said Monday.

A High Court judge told Sky, Everything Everywhere, TalkTalk, O2 and Virgin Media on Friday to prevent access to the Swedish site, which helps millions of people download copyrighted music, movies and computer games.

Music industry group BPI welcomed the order by justice Richard Arnold that the service providers block the site within the next few weeks.

BPI chief executive Geoff Taylor said sites like The Pirate Bay "destroy jobs in the U.K. and undermine investment in new British artists."

The service providers said they would comply with the order. A sixth provider, BT, has been given several weeks to consider its position, but BPI said it expected BT would also block the website.

Providers who refuse could find themselves in breach of a court order, which can carry a large fine or jail time.

Monday’s announcement follows a February ruling by the same judge that the operators and users of The Pirate Bay have "a common design to infringe" the copyright of music companies.

The Pirate Bay has been a thorn in the side of the entertainment industry for years. In 2010, a Swedish appeals court upheld the copyright infringement convictions of three men behind the site, but it remains in operation.

The website, which has more than 20 million users around the world, does not host copyright-protected material itself, but provides a forum for its users to download content through so-called torrent files. The technology allows users to transfer parts of a large file from several different users, increasing download speeds.

Defenders of such sites say old creative industry business models have been overtaken by technology that allows music, movies and games to be acquired at the touch of a finger on computers, tablets, phones and other devices.

Both O2 and Virgin said banning orders against copyright-breaching sites had to be accompanied by other measures that reflected consumers' behavior.

O2 said in a statement that "music rights holders should continue to develop new online business models to give consumers the content they want, how they want it, for a fair price."

Indictment Returned in NYC Computer Hacking Case

The name of a Chicago man already charged in a computer hacking case aimed at taking out key players in the worldwide group Anonymous was added to an indictment Wednesday, boosting the accusations against him by including him in much of the wider conspiracy to hack into corporations and government agencies worldwide.

Jeremy Hammond, 27, joined four other defendants named in the indictment in federal court in Manhattan in a prosecution revealed in March. Hammond, 27, is being held at a lower Manhattan lockup after initially appearing in a Chicago court.

Authorities said the prosecution marks the first time core members of the loosely organized worldwide hacking group Anonymous have been identified and charged in the U.S.

Prosecutors said the defendants and others hacked into companies and government agencies worldwide, including the U.S. Senate. They say they also stole confidential information, defaced websites and temporarily put some victims out of business. Authorities say their crimes affected more than 1 million people.

A message left with Hammond's lawyer for comment was not immediately returned. It was not clear when Hammond would appear at an arraignment to enter a plea to the indictment.

Hammond is the only defendant in Manhattan, except for Hector Xavier Monsegur, a 28-year-old self-taught, unemployed computer programmer who was living on welfare in public housing in New York when he joined other elite hackers in various schemes.

A legendary hacker known as Sabu, Monsegur pleaded guilty and cooperated for most of the last year with the FBI, which built the case against Hammond and four others, who were arrested in Scotland, England and Ireland. None of the others have come to the U.S. to face the charges. Extraditions were being sought.

Hammond is charged in the indictment with conspiracy to commit computer hacking, computer hacking, conspiracy to commit access device fraud and aggravated identity theft.

The indictment adds allegations that the conspiracy included a hack of

the Arizona Department of Public Safety, a state law enforcement agency in Arizona.

ICANN To Notify Domain Applicants of Data Breaches

Organizations taking part in the most ambitious expansion of the Internet so far will find out next week whether their applications for new domain names could have been viewed by competitors as a result of a software bug.

The U.S. non-profit Internet Corporation for Assigned Names and Numbers (ICANN), which operates the Internet’s naming system, has been inviting Organizations to apply to own and run their own domains, for example .apple, .nyc or .gay, instead of entrusting them to the operators of .com, .org and others.

But the system hit a problem earlier this month, just as a three-month window for applications was about to close, when a software glitch was discovered that allowed some applicants to see user or file names of other applicants.

Organizations had been careful not to reveal the domain names they were applying for, fearing the knowledge they were applying for a generic domain like .food would encourage rivals to compete for that domain and drive up the price.

"We’re very apologetic for the inconvenience to any applicants," ICANN chief executive Rod Beckstrom told Reuters.

"Clearly, we’re going to take every step that we can to make sure that no one takes advantage of any information they may have obtained," he said in a telephone interview, declining to detail exactly what steps could be taken.

The domain-name expansion programme had been opposed by some influential trademark owners who feared they would have to spend large sums of money simply to protect their brands online, despite protections built into the system.

Critics have also complained about conflicts of interest as some past and present ICANN board members stand to benefit financially from the programme.

Peter Dengate Thrush, who was chairman of ICANN when it gave the go-ahead for the expansion, went on to become executive chairman of Top Level Domain Holdings, a London-listed firm set up to acquire and operate the new domains.

Beckstrom said he was confident the glitch in the system had been caused by a software bug rather than an attack.

"We have absolutely no reason to believe it’s a hack. We have been able to find some of the instructions in the software that caused the issue," he said.

Beckstrom added that ICANN had captured every keystroke made by applicants since the window opened in January, and was currently combing through the more than 500 gigabytes of data to determine what may have been visible to

whom.

The organization plans to notify applicants by May 8 if details of their applications could have been viewed by others, but will not tell them who could have seen those details. Those who may have viewed such information will also be notified.

ICANN, which says it has now fixed the bug and is extensively testing the system, plans to reopen the application window at a date yet to be determined for an extra five days.

Beckstrom said 1,268 Organizations had registered for the application system to date, up from a previously reported figure of 839, and stressed that most applicants were not affected.

"As CEO, I take full responsibility for this issue," said Beckstrom, who is due to step down on July 1. "I would like to resolve it before handing on the baton."

Internet Group: Quality Over Speed in New Domains

The organization in charge of expanding the number of Internet address suffixes - the ".com" part of domain names - is apologizing for delays but says it’s favoring "quality, not speed."

Three weeks ago, the Internet Corporation for Assigned Names and Numbers abruptly shut down a system for letting companies and organizations propose new suffixes, after it discovered a software glitch that exposed some private data. At the time, ICANN planned to reopen the system within four business days. The system remains suspended indefinitely.

"We’ve very focused on the quality of what we do," ICANN CEO Rod Beckstrom said. "We take this very seriously. That’s why we’re moving very methodologically and professionally."

In an interview with The Associated Press this week, Beckstrom added, "We apologize for the delay, but we’re committed to getting this right."

ICANN has said it needed time to figure out why the software failed and how to fix it. That was completed last week, Beckstrom said, but ICANN still must undergo extensive testing on the fixes and inform companies and organizations whose data had been exposed. He declined to offer a timetable.

Up to 1,000 domain name suffixes could be added each year in the most sweeping change to the domain name system since its creation in the 1980s.

The idea is to let Las Vegas hotels, casinos and other attractions congregate around ".Vegas," or a company such as Canon Inc. draw customers to "cameras.Canon" or "printers.Canon." The new system will also make Chinese, Japanese and Swahili versions of ".com" possible.

After several years of deliberations, ICANN began accepting applications in mid-January. The application window was to have closed on April 12 - the same day ICANN had to shut down the system, just hours before the deadline.

The glitch did not affect general availability of the Internet’s domain name system - the databases that let Internet-connected computers know where to send email and locate websites. It also did not affect the ability to register new names under existing suffixes.

Rather, the glitch was with the software ICANN had set up to take applications for new suffixes.

The proposals were supposed to be confidential until the application period closed. The software glitch allowed some applicants to view data about others, including potential competitors. The data were limited to file names and usernames, not the contents of the files.

But those names in some cases offered clues about which companies were proposing what suffixes, Beckstrom said. Knowing that could allow an applicant to change a proposal and gain an advantage.

ICANN believes that 105 applicants might have had data viewed by others, while 50 applicants might have seen information on others - inadvertently, ICANN believes. That’s out of 1,268 registered applicants, each of which can submit as many as 50 suffix proposals.

Beckstrom said that once the system reopens, ICANN will monitor applicants to determine whether they make adjustments based on what they might have seen. Applicants will also have at least a week to make sure their data didn’t get lost or corrupted.

The delay shouldn’t have a major effect on the availability of new suffixes, as the new names won’t appear in general use until at least next spring - in many cases, much later.

The bigger damage could be in the long-term confidence in ICANN. Even before the glitch was discovered, opponents of the domain-name expansion questioned ICANN’s ability to roll out new suffixes smoothly.

Beckstrom said all organizations encounter technical problems, and he said ICANN hopes to retain people’s confidence by resolving the problems and communicating well.

Chrome 18 Is World s Most Popular Browser

Internet monitoring firm Pingdom on Monday released a new report on global Web browser share by browser version. The company found Microsoft s Internet Explorer 9 to be the most popular browser in North America with a 21.2% share, and it was closely followed by Google Chrome 18 at 20.2%. Internet Explorer, however, featured a combined total of 40.4% of the North American browser market. Globally, Pingdom found that Chrome 18 is the most popular browser with a 25.6% share, leading Firefox 11 with 15.8% and Internet Explorer 9 and 8 with 15.7% and 14.6%, respectively. Microsoft s browser has the largest worldwide market share when all versions are combined, followed by Chrome and then Firefox.

Motorola Wins Xbox and Windows 7 Ban in Germany

Motorola Mobility has been granted an injunction against the distribution of key Microsoft products in Germany.

The sales ban covers the Xbox 360 games console, Windows 7 system software, Internet Explorer and Windows Media Player.

It follows a ruling that Microsoft had infringed two patents necessary to offer H.264 video coding and playback.

A US court has banned Motorola from enforcing the action until it considers the matter next week.

The handset maker is in the process of being taken over by Google.

This is just one of several cases involving about 50 intellectual properties that the smartphone maker has claimed that Microsoft should have licensed.

Microsoft has said that if it met all of Motorola’s demands it would face an annual bill of $4bn (£2.5bn). Motorola disputes the figure.

A statement from Motorola said: "We are pleased that the Mannheim Court found that Microsoft products infringe Motorola Mobility’s intellectual property. As a path forward, we remain open to resolving this matter. Fair compensation is all that we have been seeking for our intellectual property."

Microsoft said it planned to appeal against the German ruling.

"This is one step in a long process, and we are confident that Motorola will eventually be held to its promise to make its standard essential patents available on fair and reasonable terms for the benefit of consumers who enjoy video on the web," a spokesman said.

"Motorola is prohibited from acting on today’s decision, and our business in Germany will continue as usual while we appeal this decision and pursue the fundamental issue of Motorola’s broken promise."

Microsoft moved its European software distribution centre from Germany to the Netherlands last month ahead of the verdict to minimise potential disruption.

However, Motorola cannot enforce the ruling until a Seattle-based judge lifts a restraining order.

The restriction was put in place after Microsoft claimed that Motorola was abusing its Frand-commitments - a promise to licence innovations deemed critical to widely-used technologies under "fair, reasonable and non-discriminatory" terms.

A hearing is scheduled for 7 May, although the judge may issue his ruling at a later date.

The German case is also likely to be considered by the European Commission.

It is carrying out two probes into whether Motorola’s Frand-type patent activities amount to "an abuse of a dominant market position".

EU’s Top Court: APIs Can’t Be Copyrighted, Would "Monopolise Ideas"

The European Court of Justice ruled on Wednesday that application programming interfaces (APIs) and other functional characteristics of computer software are not eligible for copyright protection. Users have the right to examine computer software in order to clone its functionality - and vendors cannot override these user rights with a license agreement, the court said.

The case focuses on the popular statistical package SAS. A firm called World Programming created a clone designed to run SAS scripts without modification. In order to do this, they bought a copy of SAS and studied its manual and the operation of the software itself. They reportedly did not have access to the source code, nor did they de-compile the software’s object code.

SAS sued, arguing that its copyright covered the design of the SAS scripting language, and that World Programming had violated the SAS licensing agreement in the process of cloning the software.

The EU’s highest court rejected these arguments. Computer code itself can be copyrighted, but functional characteristics - such as data formats and function names - cannot be. "To accept that the functionality of a computer program can be protected by copyright would amount to making it possible to monopolise ideas, to the detriment of technological progress and industrial development," the court stated.

"The purchaser of a software licence has the right to observe, study, or test the functioning of that software in order to determine the ideas and principles which underlie any element of the program. Any contractual provisions contrary to that right are null and void," the court ruled.

American courts have generally agreed with the European court’s position that functional characteristics of computer programs are not eligible for copyright protection. (But the idea is currently under debate in the high-profile legal battle between Google and Oracle. Oracle says Google violated its copyrights by cloning Java APIs for use in Android.)

But American courts have been reluctant to overrule license agreements, which often remove rights that a user would otherwise possess. For example, in 2010 the US Court of Appeals for the Ninth Circuit upheld EULA terms that prohibited reverse-engineering World of Warcraft.

After Wednesday’s ruling, European software users enjoy broader rights to clone software than do users on this side of the pond.

=~=~=~=